Networked authoritarianism and the geopolitics of information: understanding Russian Internet policy

Maréchal, Nathalie

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Empfohlene Zitierung / Suggested Citation:
Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: understanding Russian Internet policy. *Media and Communication*, *5*(1), 29-41. https://doi.org/10.17645/mac.v5i1.808

COGITATIO

Media and Communication (ISSN: 2183–2439)
2017, Volume 5, Issue 1, Pages 29–41
DOI: 10.17645/mac.v5i1.808

Article

Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy

Nathalie Maréchal

Annenberg School for Communication and Journalism, University of Southern California, Los Angeles, CA 90007, USA;
E-Mail: marechal@usc.edu

Submitted: 30 October 2016 | Accepted: 6 February 2017 | Published: 22 March 2017

Abstract
In the aftermath of the 2016 U.S. election, researchers, policymakers and the general public are grappling with the notion that the 45th president of the United States may very well owe his electoral victory to a sophisticated propaganda effort masterminded by the Kremlin. This article synthesizes existing research on Russia's domestic information controls, its internet policy at the global level (notably via internet governance processes), and the country's resurgence as a major geopolitical player to argue that policymakers as well as the general public should consider these themes holistically, particularly as they formulate responses to what many see as the Russian threat to Western liberal democracy. Russia may have lost the Cold War, but it is now waging information warfare against the liberal democracies of Europe and North America in a sophisticated bid to win the next round. Russia does not view internet governance, cybersecurity, and media policy as separate domains. Rather, all the areas covered by those disciplines fall under "information security" for Russian foreign policy. The paper begins by tracing the history of information controls within what is now the Russian Federation before discussing the role of information and internet policy in Russian foreign policy, drawing connections between the Russian government's control and manipulation of information—including its internet policy—in the domestic and international arenas. Next, it discusses the spread of networked authoritarianism and suggests that a "geopolitics of information" will become increasingly necessary in the coming years. Just as networked authoritarianism establishes strategic infrastructures to control the message domestically and intervene in global media systems, liberal democracies need to rethink media and communication infrastructures to ensure they foster pluralist, rights-respecting societies that are resilient to authoritarianism and extremism. In doing so, they should resist the temptation to respond to this threat in ways that will erode democracy even further, such as expanded surveillance and limits on free expression.

Keywords
2016 election; censorship; data localization; human rights; networked authoritarianism; propaganda; Russia; surveillance

Issue
This article is part of the issue "Post-Snowden Internet Policy", edited by Julia Pohle (WZB Berlin Social Science Center, Germany) and Leo Van Audenhove (Vrije Universiteit Brussel, Belgium).

1. Introduction

After a long and bitter electoral campaign, the results of the 2016 U.S. election have precipitated an ongoing constitutional crisis, and continued uncertainty about the role of Russia's government in Donald Trump's electoral victory has prompted renewed interest in Russia, a country that hadn't been at the forefront of the national agenda since the end of the Cold War. Several factors contribute to making the current situation a perfect storm of uncertainty and ambiguity, including: policymakers' and the public's comparative lack of knowledge about Russia; the difficulty of parsing out something resembling empirical truth from the jumble of official statements, leaks, speculations and claims made by the various actors involved; the tumultuous presidential transition; and the arcane nature of the empirical claims underlying the web of controversy surrounding the election and any role Russia might have had in influencing the result. It will take time and serious effort for the dust

to settle; an analysis of the events leading up the 2016 election, or of the election's aftermath, would be premature. However, at this stage it is appropriate to consider what we do know about Russia's policies concerning information, the internet and international relations under Vladimir Putin.

There is a natural tendency in scholarship and policy to work within disciplinary silos, without sufficiently considering related developments that are better aligned with a different field of expertise. At a time when American interest in Russia is at perhaps its highest since the end of the Cold War, it is important to consider all of Russia's information and internet policy, both domestic and international, in order to properly situate current developments and formulate policy responses that defend and support democracy and human rights. The topic is a complex one, and it would be impossible to cover it entirely, with all its nuances and complexities, in an article-length piece. My aim here is twofold: to draw connections between the Russian government's control and manipulation of information—including its internet policy—both domestically and externally, and to theorize on the spread of networked authoritarianism and the future of the geopolitics of information.

This article was written for a thematic issue on "Internet Policy After Snowden", but it is broader than that in at least two ways. First, it goes beyond narrow definitions of internet policy to consider several aspects of Russian information and communication policy that are inextricably intertwined. And second, it has very little to say about Edward Snowden. At least in the Russian context, the 2013 Snowden revelations mainly serve as a temporal marker. They alerted global public opinion to mass surveillance and made possible a change in the Kremlin's rhetoric, but did not cause a shift in Russian policy. If there was a turning point in Russian internet policy, that moment was in 2011: the year of the Arab Spring, but also the year that Russian civil society used social media to organize protests of the legislative election, about which then-U.S. Secretary of State Hillary Clinton expressed "serious concerns" (Labott, 2011). It was also the year before Putin resumed the presidency, after swapping roles with Dmitri Medvedev for four years.

In this article, I synthesize existing research on Russia's domestic information controls policy, internet policy at the global level (notably via internet governance processes), and the country's resurgence as a major geopolitical player to argue that policymakers as well as the general public should consider these themes holistically, particularly as they formulate responses to what many see as the Russian threat to Western liberal democracy. In doing so, they should resist the temptation to respond to this threat in ways that will erode democracy even further, such as expanded surveillance and limits on free expression.

Methodologically, the article relies chiefly on secondary sources, including translations of Russian sources and sources written in English by Russian journalists, while drawing on my interactions with a variety of policy experts (both Russian and Western) in the course of other ongoing work, some of whom have asked to remain anonymous for their own safety. Throughout the article I consider information policy, media policy and internet policy holistically, as they are closely interrelated. The article begins by tracing the history of information controls (which predate the internet) within what is now the Russian Federation before discussing the role of information and internet policy in Russian foreign policy. Next, I discuss the spread of networked authoritarianism and suggest that a "geopolitics of information" will become increasingly necessary as the 21st century marches on, and theorize on what this might be, concluding with a call to defend, protect and improve Western liberal democracy.

2. Information in Russia Before the Internet

This section traces the history of the media and information controls in Russia, which is distinct from the history of the press and the media in the West. Media in Russia have always served as instruments of political propaganda, going back to the country's first newspaper. *Vedomosti* was founded in 1702 to disseminate the czar's wishes, plans, and priorities across the country, and to build popular support for the ruler (Rohlenko, 2007). Under the USSR, information was considered a dangerous commodity to be feared and controlled, rather than a right and a public good. Contrary to liberal conceptions of a free press serving as a fourth branch of governance and fostering a habermasian public sphere (Habermas, 1989), the Soviet regime saw the media as a danger to be tightly controlled, with only select elites permitted access to objective news or to foreign publications (Gorny, 2007; Soldatov & Borogan, 2015). For example, ownership and use of photocopiers were tightly restricted in an attempt to prevent the distribution of *samizdat*, photocopied pamphlets of "subversive" material (Hanson, 2008).

It is no accident of history that the collapse of the USSR coincided with the emergence of the information society in the West. Indeed, Castells and Kiselyova (1995) argue that this death grip on information was the primary reason for the USSR's implosion. The 1990s were a period of relative freedom for the press in post-Soviet Russia, albeit a short-lived one as the levers of power—recently relinquished by the Communist Party—were seized by the new oligarch class. The media were no longer beholden to a monolithic ideology, but instead answered to a variety of corporate backers whose interests didn't always align. Print media lost their state subsidies and saw their circulation and importance decline precipitously, leaving broadcast TV to take over as the country's predominant communication medium (Ognyanova, 2015).

Vladimir Vladimirovich Putin, Yeltsin's chosen successor, first assumed the presidency of the Russian Federa-

tion in 1999, and quickly restored the Kremlin's control over print and broadcast media—a move that he characterized as "liberating" news outlets from the oligarchs. For many Russia experts, understanding Putin is key to understanding Russia today. Putin served in the Soviet intelligence agency, the KGB, for 16 years, rising to the rank of colonel, and he spent much of the pivotal perestroika years outside of Russia. His views on governance, the rule of law, the role of information in society, and the Russian national interest are very much influenced by the KGB's authoritarian traditions, themselves grounded in the authoritarianism of imperial Russia. Putin switched posts with his prime minister, Dmitri Medvedev, in 2008 to circumvent constitutional term limits, and in 2012 Putin returned to the Kremlin and redoubled his efforts to control the internet (Ognyanova, 2015; Soldatov & Borogan, 2015).

The end of the Cold War, which also ended Russia's superpower status (as nominal as it might have been, particularly toward the end), was a sore spot for the Russian elite, which perceived the U.S.'s success in exporting its cultural products as a threat to national sovereignty. Elites also resented growing U.S. influence in Eastern Europe and Central Asia, which they saw as their rightful sphere of influence, and the European Union's eastward expansion. Over the course of his first presidency (2000–2008), during which time domestic internet access grew considerably, Putin came to see the information revolution as "one of the most pervasive components of U.S. expansionism in the post-Soviet sphere, most notably in Russia itself" (Nocetti, 2015, p. 129). Where others might have seen opportunities for innovation and growth, Putin saw threats to the status quo and his hold on power, thus following in the footsteps of his Soviet and pre-bolshevik predecessors alike.

3. The Russian Information Controls Regime

Ronald Deibert and his team at the University of Toronto's Citizen Lab coined the phrase "information controls" to describe the "techniques, practices, regulations or policies that strongly influence the availability of electronic information for social, political, ethical, or economic ends". These include technical means like "filtering, distributed denial of service attacks, electronic surveillance, malware, or other computer-based means of denying, shaping and monitoring information" and policies like "laws, social understandings of 'inappropriate' content, media licensing, content removal, defamation policies, slander laws, secretive sharing of data between public and private bodies, or strategic lawsuit actions" (Citizen Lab, 2015). As a field of inquiry, information controls can also include the means of circumventing or otherwise countering barriers to the free flow of information online. Importantly, the field is inherently multidisciplinary and transcends the barrier between academia and civil society, with many important advances coming from activists and nonprofits.

The Freedom on the Net Index classifies information controls under three broad categories: obstacles to access, limits to content, and violations of user rights (Karlekar & Cook, 2009). Compared to China, Russia rarely uses obstacles to access (which include infrastructural and economic barriers as well as shutdowns and application-level blocking), relying instead on censorship and intimidation. However, Russia is taking steps to create an internet "kill switch", allowing it to disconnect the RuNet from the global network "in case of crisis", without specifying what such a crisis might entail beyond vague allusions to the internet being shut off from the outside (Duffy, 2015; Nocetti, 2015). Internet shutdowns—whether of all connection to the outside world, or of specific applications and protocols like VOIP, Twitter or WhatsApp—are used by governments like Egypt, Uganda and Iran to control the flow of information around elections, protests, and other politically sensitive events (DeNardis, 2014). The advocacy organization Access Now has reported a marked increase in the number of network shutdowns worldwide in recent years (Access Now, 2016). The Russian "kill switch" system has yet to be put into effect, as of this writing.

Censorship and violations of user rights, then, have historically been the principal mechanisms for information control in Russia. Katherine Ognyanova (2015) identifies three mechanisms through which the Russian state asserts power over the media: censorship and resulting chilling effects, state control over mainstream (especially broadcast) media, and the selective application of unrelated laws (building codes, tax laws, criminal laws, and intellectual property laws have all been used for this purpose) to put pressure on media organizations as well as individual journalists, bloggers, and activists. Extrajudicial executions are not uncommon. This is in many ways a continuation of the mechanisms used by successive Russian and Soviet governments to control the traditional print and broadcast media (Ognyanova, 2015). One key difference from the Soviet era is that the domestic media has since been privatized, and foreign companies—notably internet intermediaries—now operate in Russia as well.

In Russia, as in most countries, the physical structure of the internet is built, owned and maintained by the private sector. Companies like internet companies, Internet Service Providers (ISPs), social networking sites (SNSs), search engines, blogging platforms, and more then exercise a form of de facto private governance over online activity (MacKinnon, 2012). This private rule-making can come into conflict with the law. Absent a strong rule of law, governments can use their power to constrain, influence and even coerce information and telecommunications (ICT) companies. As Laura DeNardis notes, "state control of Internet governance functions via private intermediaries has equipped states with new forms of sometimes unaccountable and nontransparent power over information flows" (DeNardis, 2014, p. 15). We now turn to an examination of how the Russian state practices cen-

sorship and surveillance with the assistance of the private sector.

4. Censorship

Media in the Russian Federation, including the internet, is regulated by a branch of the Ministry of Communications and Mass Media, the Federal Service for Supervision of Communications, Information Technology, and Mass Media, better known as Roskomnadzor. Unlike the UK's Ofcom or the U.S. Federal Communications Commission, which are independent agencies with no power of prior restraint (the main enforcement mechanism is to assess fines), Roskomnadzor can block certain types of content without a court order: calls for unsanctioned public actions (i.e. protests), so-called extremist content, materials that violate copyright, information about juvenile victims of crime, child abuse imagery, drug propaganda, and information about suicide—as can several other agencies, including the Federal Drug Control Service, the Federal Service for Surveillance on Consumer Rights and Human Wellbeing, and the Prosecutor General's Office (Freedom House, 2015). Other types of content can also be blocked, but a court order is required.

While the authority to censor rests with the state, the responsibility to implement censorship falls on the internet service providers, who are held legally responsible for any forbidden content that is accessible to their users, a legal construct known as intermediary liability (MacKinnon, Hickock, Bar, & Lim, 2014). Since 2014, the Russian media regulator Roskomnadzor has maintained a block list of websites featuring banned content, including child abuse imagery, drug-related content, and "suicide advocacy". ISPs must regularly consult this "blacklist" of verboten websites, and are incentivized to interpret blocking orders as widely as possible to avoid liability for under-censoring, which can result in heavy fines and even the loss of their state licenses. The "blacklist" itself is often vague as to which page within a website or service should be blocked, or only specifies an IP address—which can represent any number of websites. Crucially, the list itself is secret, leaving internet users in the dark as to what is actually prohibited (Freedom House, 2015, 2016).

Roskomnadzor's powers are even greater with respect to websites that are registered as mass media—a broader category than one might think, thanks to the "Bloggers' Law". As early as 2001, the then-press minister, Mikhail Lesin,[1] "called for legislation requiring the registration of Internet media outlets", which would have included any website registered with the .su or .ru top-level domain (TLD) (Ulmanu, 2001, as cited in Bowles, 2006). Lesin finally got his wish in 2014, when the so-called "Bloggers Law" was instituted, requiring all online outlets (including blogs and personal pages within social networking sites) with more than 3,000 daily page views to register with the government, while the "Law Against Retweets" punishes the dissemination or re-dissemination of "extremist content" with up to five years in prison. "Extremist content" is defined so vaguely that it can be interpreted to include many kinds of speech that would be considered innocuous in many other countries. Another 2014 law prohibits the use of public wifi without providing one's mobile phone number. Acquiring a SIM card, in turn, requires providing one's passport number, as does signing up for home internet access. It is all but impossible, then, to surf the "RuNet" (as the Russian-language internet is called) without linking one's online activity to one's identity and passport (Duffy, 2015).

Under Article 4 of the law "On Mass Media", the regulator can issue warnings to an outlet's editorial board about "abuse of freedom of mass media", a category that includes such infractions as obscene language, information about illegal drugs, extremism, incitement to terrorism, and propaganda and cruelty. Here again, the specific interpretation of these terms leads to censorship well beyond what a literal reading of the law might suggest. For example, news sites have received warnings for publishing stories about calls for greater local governance ("federalization") and for government reform, and about international news events related to freedom of expression such as the attack on the Charlie Hebdo offices in Paris in January 2015 (Freedom House, 2015).

In addition to legislative and technical controls, the flow of information on the Russian internet is limited by two "soft" factors: cultural norms and practices grounded in centuries of authoritarianism, and deliberate framing of the internet as dangerous (Ognyanova, 2015). The Russian political class and broadcast media work together to frame the internet as a dangerous place, and online content as "unreliable, biased, and dangerous" (Kratasjuk, 2006; Ognyanova, 2015). For example, the mayor of Moscow wrote that "propaganda of drugs and violence, human trafficking and child prostitution—that's the reality of today's internet", asserting that "the Internet is gradually being settled by unconcealed terrorists who turn the web, not only into their own mailbox, but into a real, underground, military infrastructure" (Ognyanova, 2015). The strategy seems to be effective. Indeed, the report "Benchmarking Public Dissent: Russia's Appetite for Internet Control" found that 49% of all Russians believe that information on the internet needs to be censored, while 42% of Russians believe foreign countries are using the internet against Russia and its interests, and 24% think the internet threatens political stability (Nisbet, 2015). Propaganda of the kind described above allows the Kremlin to present its restrictions on the free flow of information as responses to popular will.

Restrictions on free expression continue apace, as the 2016 Yarovaya laws place new restrictions on "proselytizing" (i.e. discussing one's religion with potential converts) and require anyone with knowledge that someone else is "planning" certain kinds of crimes, mainly offenses

[1] Lesin was found dead, seemingly of a blow to the head, in a Washington hotel in November 2015. See Smith and Walker (2016).

that involve expressing dissenting views, to notify the authorities (Lokshina, 2016).

5. Surveillance

Domestic surveillance in Russia predates the internet, of course. As with censorship, the current surveillance regime is historically grounded in the country's Soviet and imperial past. The KGB may have a new acronym, FSB (standing for Federal'naya sluzhba bezopasnosti, or Federal Security Service), but it casts a long shadow (Soldatov & Borogan, 2015).

The System of Operational-Investigatory Measures (SORM) was first implemented in 1995, requiring telecommunications operators to install FSB-provided hardware allowing the agency to monitor users' communications metadata and content—including phone calls, email traffic and web browsing activity, despite the low internet penetration rate at the time.

Coming in the final year of Yeltsin's presidency, the 1999 SORM-2 reform required the FSB to obtain a post-collection court warrant to access records (Bowles, 2006). This was an encouraging sign that the intelligence services of the new Russian Federation would be governed by the rule of the law. However, shortly after taking office, Putin authorized several additional agencies to access SORM's collected data, including the tax authorities, border patrol and customs agencies, and the Presidential Security Service. The warrant requirement remains in place, but is remarkably toothless: surveillance can begin before the warrant is granted (or even requested), the warrant need not be shown to anyone (whether the surveillance target or the telecom operator), and it is only required for the retrieval of collected communications content, and not for the metadata that is often just as revealing as content, if not more so. In 2012 SORM-2 was expanded to include social media platforms, though documentation of how this works in practice is scant (Paganini, 2014; Soldatov & Borogan, 2012, 2015). Nevertheless, the assumption among Russian digital rights activists is that any information shared on Russian social networks like Vkontakte or Odnoklassniki is collected by the intelligence services (author interviews, 2016).

The latest update to SORM came in 2014, when the Ministry of Communications ordered companies to install new equipment with Deep Packet Inspection (DPI) capability (Soldatov & Borogan, 2015). As DeNardis puts it, "DPI is a transformational technology that creates unprecedented regulatory possibilities for controlling the flow of content online" (2014, p. 206). Demonstrating why this is the case requires a basic understanding of the technology itself. Information (whether it's text, voice, or something else) is transmitted over the internet as packets, small bundles of data that are individually routed from the sender to the receiver, then put back together in the correct order. Packets consist of both payload (the actual content of the communication) and a header, which contains the packet's metadata: its origin, destination, and not much else. The header is analogous to an envelope, telling each piece of equipment along the way where the payload should be delivered. Until fairly recently, computing power limited the types of analyses that routers, switches and other network hardware could perform on passing traffic, but advances in this domain have made it possible for hardware to simultaneously process millions of packets, reading not just the headers but the payload as well. Unless the packet is encrypted, the only impediment to stopping a DPI-capable machine from reading the payload are social and legal norms against this type of surveillance—which are absent in Russia. From there it is possible to block or throttle back traffic based on its origin, destination, file type (text, voice, multimedia), protocol (P2P, FTP, HTML, SMTP) or the content of the message itself (DeNardis, 2014). Here again, there is little reliable, publicly available information on how SORM-3 works, as discussing the topic is against the law. The new, secret regulations came into effect in fall 2016, and apply to all ISPs in Russia. Noncompliance comes at a steep price: stern warnings from Roskomnadzor followed by revocation of the ISP's license. Extra-legal intimidation is common, and formal enforcement appears to be increasing. Indeed, investigative journalists Andrei Soldatov and Irina Borogan obtained internal Roskomnadzor statistics that showed that the number of warnings issued by the agency grew from 16 in 2010 to 30 in 2012 (Soldatov & Borogan, 2013).

Also in 2012, SORM was applied to social networking sites, a key area of concern for Russian authorities given the role of such sites in various "color revolutions" and the 2011 Arab Spring (Howard & Hussain, 2013). As Soldatov and Borogan note, the tools used to monitor social networking sites had a crucial flaw:

> These systems were developed for searching structured computer files, or databases, and only afterwards adapted, some more successfully than others, for semantic analysis of the Internet. Most of these systems were designed to work with open sources and are incapable of monitoring closed accounts such as Facebook.
>
> The FSB discovered early on that the only way to deal with the problem was to turn to SORM. The licenses require businesses that rent out site space on servers to give the security services access to these servers via SORM, without informing the site owners. With this provision, the FSB has had few problems monitoring closed groups and accounts on Russian social networks Vkontakte and Odnoklassniki. But Facebook and Twitter don't store their user data in Russia, keeping it out of SORM's reach. (Soldatov and Borogan, 2013, para. 20)

Edward Snowden's revelations about the U.S. National Security Agency's PRISM program, which tapped into American ICT companies' data centers to extract desired

information, provided the perfect justification for requiring all data pertaining to Russian citizens to be stored within the Russian Federation. Brazil and several European countries have made announcements about eventual data localization requirements, as well, providing further legitimacy to the Russian plan in the eyes of public opinion. However, there is no evidence that data localization does much to protect user privacy (Sargsyan, 2016). Indeed, it is much easier (and more clearly within the bounds of U.S. law) for the U.S. intelligence apparatus to target data outside of the U.S., while locating data centers within Russia makes it easier for Russian agencies to access user content. Data localization serves to increase the Kremlin's access to citizen data under the guise of protecting the Russian public from American spies.

The 2016 Yarovaya laws further expanded the government's surveillance powers by increasing the mandatory data retention period to six months for content and three years for metadata and mandating cryptographic backdoors in all messaging applications (Lokshina, 2016).

6. Conscripting the Private Sector

Twenty-first century information controls in Russia distinguish themselves from earlier systems of repression in two key ways: the introduction of ICT technologies, and the irruption of the private sector in what was previously a totalitarian, state-controlled ecosystem. Moscow's appetite for surveillance has grown apace with the potential targets provided by widespread ICT adoption, and the FSB-oligarchic alliance that dominates both the state and the economy excels at finding ways to pressure ICT companies to provide the needed access to data flows.

A 2013 study by the now-defunct Center for the Study of Media and Society at the New Economic School in Moscow[2] sought to ascertain the policies and mechanisms used by domestic Russian ICT companies to protect the digital rights of their users. Conducted during a time of great uncertainty for the ICT sector in Russia, the study found that company representatives were hesitant to discuss issues of human rights (preferring the term "user rights"), the pressures they faced from the Kremlin, or the possibility of doing anything other than following the law. The majority of companies reported that they comply with all demands from the government, while only a few seemed to try to negotiate these demands. All of the companies surveyed reported being sensitive to government demands and having to contend with censorship issues, all the while insisting that they adhered to high standards of privacy and security (Maréchal et al., 2015; Petrova, Fossato, Indina, Dokuka, & Asmolov, 2013).

The Russian government ensures the compliance of domestic companies in particular by holding them liable for banned, copyrighted or otherwise illegal content accessible through their services or platforms. This intermediary liability strongly incentivizes ICT companies to block or remove any content that might plausibly be deemed illegal, lest they suffer grave repercussions (Petrova et al., 2013). Indeed, protection rackets and related thuggery are endemic in Russia, and business owners can find themselves targeted for prosecutions of dubious legal merit simply because they have upset the wrong oligarch or FSB operative (Pomerantsev, 2014). Legal remedies are nonexistent in these cases, leaving submission and exile as the only viable options. The current context of quick legislative reform and uneven enforcement keeps companies—and their staff—in a state of constant uncertainty about the rules and the penalties for breaking them.

Foreign companies operating in Russia typically have deeper pockets, greater technical and managerial know-how, and reduced vulnerability to physical threats compared to their domestic counterparts. Google closed its Russian engineering offices in late 2014 (Luhn, 2014), and a number of former high-level executives have left the country (author interview, 2016). Neither Facebook nor Twitter have offices in Russia (Masnick, 2014), and without local staff who could face retaliation, the American platforms have greater leeway to push back against demands for censorship or for user information. According to Twitter's Transparency Report, the company refused to comply with any of the 233 requests for user information it received from Moscow in 2014–2015 (Twitter, 2015, 2016), and complied with only 5% of takedown requests received in the second half of 2015 (Twitter, 2016). Similarly, Google only produced user information for 5% of Russian government requests in the first half of 2015, though it complied with 62% of takedown requests during that period (Google, 2016). Facebook didn't comply with any Russian requests for user information, and restricted 56 pieces of content. The company does not disclose the number of requests for content restriction it received (Facebook, 2016).

Unlike domestic Russian companies, Google and Facebook (though not Twitter) are members of the Global Network Initiative, employ legal teams and other experts dedicated to advancing their users' digital rights, and engage in public transparency reporting about these issues. These efforts should be supported and encouraged. But if these companies comply with data localization laws, their users' data will fall into SORM's net, particularly given SORM-3's more powerful DPI capabilities. If they refuse, Roskomnadzor may very well block the sites entirely, as at least some of its officials have wanted to do for years (Masnick, 2014).

LinkedIn became the first foreign social media company to be banned from Russia, in part due to noncompliance with the data localization law. Roskomnadzor had sued the social networking site, which was ac-

[2] The Center received much of its funding from Western charitable foundations, which it is now prohibited from doing under the Russian law on "foreign agents". Unsurprisingly, the Center has not been able to identify domestic sources of funding, and much of its former staff is now living in the West (author interview, 2016).

quired by Microsoft earlier in 2016, for illegally sharing the personal data of non-users without obtaining prior consent—a claim that, if true, would indeed put LinkedIn afoul of data management best practices. The suit also argued that LinkedIn did not comply with data localization requirements. In its August 4, 2016, ruling, the court ordered Russian authorities to "take steps" to limit access to the site, though as of late October it remained accessible to most users (Rothrock, 2016). LinkedIn lost its appeal in November, and Roskomnadzor required Apple and Google to remove the LinkedIn app from the Russian versions of their respective app stores (Kang & Benner, 2017; Scott, 2016). With Roskomnadzor due to begin proactively enforcing foreign companies' compliance with data localization in 2017, the decisions of U.S. ICT companies like Google, Facebook and Twitter will be a test of the firms' commitment to user privacy and freedom of expression.

7. Russian Information and Internet Policy at the International Level

Russian internet policy—in both the domestic and foreign policy spheres—is rooted in the premise that Western countries (mainly the U.S.) use the internet to overthrow governments in "countries where the opposition is too weak to mobilize protests" (Nocetti, 2015, p. 114)—or, in other words, countries living under authoritarian regimes. Russian foreign policy hews to a strict interpretation of Westphalian nation-state sovereignty, at the core of which is the principle of non-intervention.[3] The free and open internet threatens that principle, allowing foreign and potentially subversive viewpoints to circulate across Russia. The "color revolutions" of the early 21st century and the Arab Spring have further fueled concerns that the internet represents a threat to the status quo and that it poses a threat to Russian political leaders (Nocetti, 2015). Indeed, opposition groups led by Alexei Navalny used Facebook to coordinate street protests in the aftermath of the 2011 legislative elections, and while the protests failed to coalesce into a lasting social movement, such an outcome was not completely outside the realm of possibility (Soldatov & Borogan, 2015; White & McAllister, 2014). Moreover, there is good reason to believe that Putin sees the U.S., and specifically then-Secretary of State Hillary Clinton, as directly responsible for fomenting these protests. Under this paradigm, such interference in Russia's domestic politics constitutes a violation of national sovereignty tantamount to information warfare. Likewise, U.S. policy initiatives like democracy promotion and the Internet Freedom Agenda are seen as promoting political projects that are aligned with U.S. interests, almost invariably at the expense of Russia's own interests (Nocetti, 2015).

Digital rights and the free flow of information are thus doubly threatening to the Kremlin. Not only does the internet embolden and empower the domestic opposition, it is (from Putin's perspective) closely associated with the U.S. government, which has historically played a unique role in internet governance and is a major funder of the global digital rights movement. In Russia's Westphalian view of the world, nation-states are the only actors that matter, and that should matter, and the actions of all other actors (be they individuals, civil society organizations, or corporations) can be imputed to a government motivated by the accumulation of power. That is the logic behind the 2012 law "On foreign agents", which stigmatizes internationally-funded NGOs that criticize the Kremlin by labelling them as "traitors" or "spies" (Human Rights Watch, 2017).

The Kremlin responded to what it sees as an existential threat by launching a campaign to reshape its near-abroad in its image, most dramatically in Estonia and Ukraine. The European and American response was tepid, and Putin grew bolder. Before long, the Kremlin was providing financial and ideological support to far-right parties and movement across the European Union, including Viktor Orbán in Hungary, the Brexit "Leave" campaign, and pro-Russian candidates in Bulgaria and Moldova (Eichenwald, 2017; Oliphant, 2016). A transnational, neo-fascist, authoritarian movement grounded in ethno-nationalism was taking shape. And then, of course, there is Donald Trump. Early analysis suggests that Trump was initially no more than a "useful fool" to be used to discredit Hillary Clinton and cast doubts on her legitimacy as president, but after a series of astounding events, the election, of course, went another way. The 2017 elections in France and Germany will be the next tests.

French Russia expert Julien Nocetti (2015) argues that "Moscow is crucially involved in the politicization of global cyber issues, to a large extent owing to the inextricable interweaving of the Russian Federation's domestic and external affairs" (p. 112). He stresses that:

> The slogan "content as threat" encapsulates the Russian perception that digital technologies can be used as tools *against* Russia. In Russian documentation it is expressed more fully as the "threat of the use of content for influence on the socio-humanitarian sphere". The notion of content as threat is reinforced by the projection onto foreign partners of Russia's own preconceptions of how international relations work, and by the presumption that a primary aim of western powers is to disrupt and undermine Russia. (p. 116)

For many years, Russia simultaneously sought to constrain the use of this powerful weapon (information) through international norms and treaties even as it developed its own offensive capabilities, echoing its Cold War approach to nuclear weapons. Since 1998—shortly before Putin became president—Russia has proposed

[3] A Westphalian paradigm doesn't mean that a country won't interfere in another country's affairs; it means that any such intervention is considered an act of war.

annual UN resolutions prohibiting "information aggression", which Nocetti interprets to mean the use of ideas or ideology to undermine regime stability (2015, p. 122). This is only one example of Russian attempts to regulate the use of information under international law. At the same time, Russia uses the Shanghai Coordination Organization (SCO) to provide technical assistance and knowledge transfer to other illiberal regimes eager to up their information controls game. This authoritarians' club further includes China, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan, with several other countries having observer or dialogue partner status. Russia and China use the SCO to share new advances in repression with one another, as well as with the less powerful member states whose regimes they want to bolster (Diamond, Plattner, & Walker, 2016; Nocetti, 2015).

8. Edward Snowden

More than three years after his initial revelations, Edward Snowden's continued asylum in Russia remains perplexing for many observers, some of whom speculate that the former NSA contractor must be a Russian agent, even if a reluctant one. The Snowden camp categorically denies this, and available evidence strongly suggests that Snowden's arrival in Moscow was not of his own making. Shortly after coming out to the world as the source for the Guardian and Washington Post stories about NSA surveillance, Snowden left Hong Kong for Latin America, with a layover in Moscow. He was accompanied by WikiLeaks's Sarah Harrison, who was apparently sent by Julian Assange to help escort Snowden to safety. There are only so many options for this route, and Moscow seemed to pose the fewest risks of being intercepted by U.S. officials. Unfortunately for Snowden, his passport was revoked while he was in the air, and he was stuck within the Moscow airport for 39 days while his asylum application was processed. Snowden was granted temporary asylum in Russia for a year, followed by a three-year residency permit in 2014 that was later extended to 2020 (Greenwald, 2014; Harding, 2014; Sharkov, 2016; Williams & Toropin, 2017).

As the world grappled with the unprecedented revelations of U.S. spying, and the key role played by internet platforms and telecommunications companies in collection programs like PRISM, governments explored ways to protect their citizens from the NSA's reach. Data localization schemes were proposed by countries as varied as Brazil, China, France, Germany, South Korea and Russia with the stated aim of ameliorating privacy risks from foreign surveillance. But in Russia at least, data localization laws "leveraged the public outrage and the heightened privacy concerns caused by the NSA spying to extend their control over data and their surveillance potential by data localization" (Sargsyan, 2016). The Kremlin thus seized the Snowden revelations, as well as his presence in Moscow, as an opportunity to craft a narrative that furthered its political objective: to portray the U.S. and its allies as the real adversaries of privacy and individual autonomy while continuing to intensify domestic censorship, surveillance, and the dismantling of Russian civil society. Meanwhile, Snowden has been an outspoken critic of Russian policy (Nechepurenko, 2016).

9. Analysis: Understanding Russia's Networked Authoritarianism

The key to understanding Russian internet policy is that it is part and parcel of an overall information control policy, the goal of which is the accumulation of power and wealth for Russia's kleptocratic elites. The global practice of information controls has undergone three generational shifts in rapid succession (Deibert, Palfrey, Rohozinski, & Zittrain, 2010). First generation controls prevent the population from accessing forbidden content, either through barriers to access or by blocking specific websites or pages. China's "Great Firewall" is a classic example of first generation information controls, and the Roskomnadzor blacklist is a poorly executed example of the same. The second generation involves creating legal and technical frameworks allowing public and private authorities to deny access to information on a case-by-case basis. "Just-in-time" blocking and sporadic internet shutdowns linked to specific political events exemplify this method. Third-generation controls combine legal and technical means with a proactive public relations (or propaganda) strategy: "it is less a matter of refusing access as of competing with potential threats through effective counter-information campaigns which discredit or demoralize the opponent" (Deibert et al., p. 16). The Kremlin's army of online trolls and use of broadcast and online media for domestic and external propaganda exemplify such third-generation controls. Deibert further identifies advocating for illiberal practices in internet governance arenas as a possible fourth generation of information controls (Deibert, 2016). This is already a core part of Russian foreign policy, as discussed above. The result is "networked authoritarianism" (MacKinnon, 2011), a political system that leverages ICTs and media regulation to carefully control the expression of dissent in a way that gives the impression of limited freedom of expression without allowing dissent to gain traction. Russia has long been "on the cutting edge of techniques aimed to control online speech with little or no direct filtering" (p. 43).

While historically Russia has indeed eschewed the more heavy-handed information controls in favor of second- and third-generation tactics, since Putin's 2012 return to the presidency—preceded by popular demonstrations that shared many characteristics of successful "color" revolutions (White & McAllister, 2014)—there have been increasing signs that the gloves are coming off. Google chairman Eric Schmidt worried as early as 2013 that Russia was beginning to copy China in internet censorship (Luhn, 2014), while SORM-3 and data localization requirements (including the LinkedIn ban) are

further indications that the Kremlin is serious about controlling information within its borders. At the international level, Russia is normalizing and helping to spread networked authoritarianism through various strategies in internet governance fora, at the UN, and through the Shanghai Cooperation Organization "authoritarians' club" (see Pearce & Kendzior, 2012, for an examination of networked authoritarianism in Azerbaijan). At the same time, it has been waging a slow, covert campaign to dismantle the transatlantic alliance using "information weapons" honed in its near-abroad, most famously in Ukraine but also in Moldova. If information has always been political, today it is geopolitical and weaponized.

If true, the allegations of Russian interference in Western elections, including the 2016 U.S. presidential contest, would clearly constitute a pattern of "information aggression". Russia may be trying to give its adversaries a taste of as their own medicine (as the Kremlin sees it), or it may be teaching the world an object lesson on the dangers of the free flow of information. It is also possible that having failed to garner support for a norm against informational violations of state sovereignty, Russia decided to use that powerful weapon to reshape the international system to better fit its authoritarian, Westphalian worldview. Regardless of the grand strategy pursued by Putin, the tactics used insidiously turned open societies' strengths—pluralism, free expression, acceptance of diversity—against them at a time when they were especially vulnerable. Indeed, in the aftermath of the 2008 financial crisis the economic recovery has left too many behind, for which many Americans blame coastal elites and the incumbent Democrats. Populist contestations of capitalism, including the surveillance capitalism that powers the internet economy (Zuboff, 2015), open a door for competing political projects like the far-right ethno-nationalisms gaining ground across Europe and, of course, the Trump phenomenon—itself no stranger to xenophobia and white supremacist themes. Liberal democracies' policy responses must navigate between Scylla and Charibdis, facing down the threat of far-right extremism without developing our own version of networked authoritarianism.

10. Towards a Geopolitics of Information

As early as 2012, Rebecca MacKinnon predicted that "in the twenty-first century, many of the most acute political and geopolitical struggles will involve access to and control of information" (2012, p. XXV). Geopolitical debates about the flow of information typically pit champions of free expression and access to information against those who want to see state sovereignty replicated in cyberspace. There are shades of gray between those positions, of course, but it is nevertheless an ideological division that should be taken seriously. As Shawn Powers and Michael Jablonski note in their book about the Internet Freedom Agenda:

> The real cyber war is not over offensive capabilities or cybersecurity but rather about legitimizing existing institutions and norms governing Internet industries in order to assure their continued market dominance and profitability….While heavy-handed government controls over the Internet should be resisted, so should a system whereby Internet connectivity requires the systematic transfer of wealth from the developing world to the developed. (Powers & Jablonski, 2015, p. 24)

Powers and Jablonski thus identify two internet-mediated threats to human wellbeing: information controls (Crete-Nishihata, Deibert, & Senft, 2013) and surveillance capitalism (Zuboff, 2015). The former represents a threat from the state, while the latter is best understood as a threat from capitalism. This article has described a third threat: information warfare, a threat from external adversaries who strategically use information to achieve geopolitical goals—or, as defined by the former head of the Directorate for Electronic Warfare of the Russian Main Naval Staff, "securing national policy objectives both in peacetime and in wartime through means and techniques of influencing the information resources of the opposing side" (Pomerantsev, 2016, p. 181).

However, it is important not to succumb to false equivalencies that equate civic activities (like teaching people how to run elections) with the present moment—the stuff of dystopian science fiction. U.S. democracy promotion and the Internet Freedom Agenda undoubtedly support regime change in a number of countries by bolstering alternative political projects (author interview with Daniel Sepulveda, 2015), however that is far from being the only reason for supporting fair elections or the open internet. In many cases, the U.S. is less interested in supporting a specific alternative to the incumbent regime than it is in opening markets for U.S. companies, and many individual policymakers and bureaucrats genuinely embrace the ideals of access to information, free expression, and accountable democracy (Powers & Jablonski, 2015). Moreover, there is no evidence that domestic demands for free and fair elections, or a free and open internet, are anything other than genuine, including in Russia.

The past several years have seen a shift from a normative debate between the "free flow" and "online sovereignty" camps, to carefully plotted intervention. President Barack Obama noted in a 2009 speech that "the great irony of the information age" is that "those states that have most successfully adopted and exploited the opportunities afforded by the Internet are also the most vulnerable to range of threats that accompany it" (Carr, 2016, p. 2). Indeed, the Russian campaign's two greatest ostensible victories to date, the British "Brexit" vote and Donald Trump's victory, took place in deeply connected societies. If politics is war by other means, then we might call this terrorism by other means. Like terrorism, information warfare turns open societies against

themselves, creating chaos and breeding suspicion. Without knowing friend from foe, or credible analysis from "fake news", societies become paralyzed, unable to coordinate against a shape-shifting enemy that many doubt is even there. For scholar Madeline Carr, "No previous technology has been regarded concurrently as a source of power and vulnerability in quite the way that the Internet has" (Carr, 2016, p. 2).

Monroe Price's (2015) examination of "the new strategic communication" provides a useful framework for understanding the new geopolitics of information. The concept almost seems tailor-made for the current crisis: strategic communication is a "consolidating relationship between information and power" that is "heavily subsidized, usually transnational, engineered and often deceptive" (p. 7), and it is "sensitive to the particular environment in which the information intervention takes place" (p. 9). This describes Russian intervention in Western elections perfectly. Price argues that the affordances of ICTs have "raised the consequences and possibilities of strategic communication to new levels" (p. 1), empowering states to "experiment with ways to 'move the needle' of public opinion among targeted populations utilizing advanced tools of communication and [to] integrate the consequences in their theories of speech and conduct" (p. 3). Having failed to secure an international agreement circumscribing transnational communication, Russia resolved to use "information weapons" first in the pursuit of its strategic objectives, with apparent success.

At least part of that success can be traced to the state of our media ecosystem. Before Facebook launched in 2005, "the often unstated assumption was that [information intermediaries like newspapers and television networks] would function (or would be obligated to function) as guardians of the public interest" (Price, 2015, p. 35). The system was far from perfect, but by and large media institutions took their gatekeeping role seriously, and followed a highly developed code of journalism ethics.

Today's intermediaries have no such ethical code, and some explicitly reject a sense of responsibility for their platforms' impact on society, as Facebook's Mark Zuckerberg did at several points during the 2016 U.S. presidential campaign (Zuckerberg, 2016). Further complicating matters, the most visible intermediaries have a global footprint: how does a profit-seeking corporation, lacking any appetite to perform journalistic functions, determine what is in the best interest of humanity?

Meanwhile, traditional media outlets have lost advertising revenues and audience shares to social media platforms, and in their weakened financial state have been absorbed by vertically integrated media conglomerates motivated by financial gain (McChesney, 2013; Pickard, 2014, 2017). The quality of discourse suffers, and the public struggles to parse truth from falsehood, opinion from fact. The "marketplace of ideas" is flooded with mediocre fare that anyone can access for free. Journalists struggle to make a living, and would-be members of the Fourth Estate flock to careers in public relations. The "quality control" on the public sphere erodes inexorably, leaving public discourse vulnerable to manipulation.

Price introduces the concept of "strategic architectures", which he defines as "large-scale efforts to fix or stabilize the relationship of states and other major players to information flows" (p. 9):

> These wholesale approaches include active rethinking of communications structures by powerful states so as to maintain control over their own narratives and affect relevant communications systems outside their borders. These are designs not only of government but of the corporate empires for whom communication is key and certainly for the media companies themselves. For those who seek to ensure a particular narrative—for example, of governmental legitimacy, religious authenticity, or the advantages of consumerism—establishing an infrastructure they can control is significant. (Price, 2015, pp. 9–10)

As John Gilmore said in 1993, the free and open global internet treats censorship as damage and routes around it, presenting a threat to networked authoritarianism. The threat would have been even greater if it had been embraced and promoted by a hegemonic power, as would doubtless have been the case under a Hillary Clinton presidency. The Kremlin saw undermining her presidency, and Americans' faith in democracy, as a geopolitical imperative, and established a strategic infrastructure to spread messages that would favor her opponent, Donald Trump, whose authoritarian predisposition, ignorance of global affairs, and business ties to Russia further increased his value as a "useful fool" (Davidson, 2016; Miller & Entous, 2017) The early days of the Trump presidency show no indication that the 45th president will respect, much less support, a free press or open internet.

11. Conclusion

The brewing conflict between Vladimir Putin's regime and the liberal democracies of Europe and North America appears to pit two conflicting paradigms about the role of information—distributed via the internet—in society (Zuboff, 2015). This article has described Russia's historical and contemporary approaches to controlling the flow of information, both domestically and at the international level, to argue that Russia does not view internet governance, cybersecurity, and media policy as separate domains. Rather, all the areas covered by those disciplines falls under "information security" for Russian foreign policy. Domestic surveillance, content censorship and illiberal internet governance reform are deeply connected to misinformation campaigns abroad, and are used strategically to achieve geopolitical goals.

Despite all its flaws, liberal democracy is still the best form of governance available if the goal is to ensure human rights and economic prosperity. Just as networked

authoritarianism establishes strategic infrastructures to control the message domestically and intervene in global media systems, we need to rethink our media and communication infrastructures to ensure they foster a pluralist, rights-respecting society that is resilient to authoritarianism and extremism. Governments, corporations, civil society organizations and the public all have roles to play in this endeavor.

Moreover, the liberal democracies of Europe and North America need significant reforms to fulfill their promises to their citizens if they are to survive. In the U.S., Barack Obama's presidency was a solid, albeit imperfect, start that a majority of voters endorsed by voting for Hillary Clinton. Scholars of all disciplines should consider how their work can support the positive reforms that our democracies urgently need, counter the forces of authoritarianism, and actively participate in the shared work of governance.

Acknowledgements

The author gratefully acknowledges Griffin Boyce, Sergei Hovyadinov, Priya Kumar, Jeff Landale, Tanya Lokot, Rebecca MacKinnon, and Sarah Myers West for their comments at various stages of this manuscript, as well as the issue editors and anonymous reviewers.

Conflict of Interests

The author declares no conflict of interests.

References

Access Now. (2016). *#KeepItOn*. Retrieved from https://www.accessnow.org/keepiton

Bowles, A. (2006). The changing face of the RuNet. In H. Schmidt, K. Teubener, & N. Konradova (Eds.), *Control + shift. Public and private usages of the Russian internet* (pp. 21–33). Norderstedt: Books on Demand.

Carr, M. (2016). *US Power and the internet in international relations*. New York, NY: Palgrave Macmillan.

Castells, M., & Kiselyova, E. (1995). *The collapse of Soviet communism: A view from the information society*. Los Angeles, CA: Figueroa Press.

Citizen Lab. (2015). *Citizen Lab summer institute*. Retrieved from http://citizenlab.org/summerinstitute

Crete-Nishihata, M., Deibert, R., & Senft, A. (2013). Not by technical means alone: The multidisciplinary challenge of studying information controls. *IEEE Internet Computing*, *17*(3), 34–41. doi:10.1109/MIC.2013.29

Davidson, J. D. (2016, August 31). Russia's cyber warfare has bigger aims than electing Donald Trump. *The Federalist*. Retrieved from http://thefederalist.com/2016/08/31/russias-disinformation-operations-aim-to-undermine-american-democracy

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds.). (2010). *Access controlled: The shaping of power, rights, and rule in cyberspace*. Cambridge, MA: MIT Press.

Deibert, R. (2016). Cyberspace under siege. In L. Diamond, M. F. Plattner, & C. Walker (Eds.), *Authoritarianism goes global: The challenge to democracy* (pp. 198–215). Baltimore, MD: Johns Hopkins University Press.

DeNardis, L. (2014). *The global war for internet governance*. New Haven, CT: Yale University Press.

Diamond, L. J., Plattner, M. F., & Walker, C. (Eds.). (2016). *Authoritarianism goes global: The challenge to democracy*. Baltimore, MD: Johns Hopkins University Press.

Duffy, N. (2015). *Internet freedom in Vladimir Putin's Russia: The noose tightens*. Washington, DC: American Enterprise Institute.

Eichenwald, K. (2017, January 10). Trump, Putin and the hidden history of how Russia interfered in the U.S. presidential election. *Newsweek*. Retrieved from http://www.newsweek.com/trump-putin-russia-interfered-presidential-election-541302

Facebook. (2016). *Global government requests report*. Retrieved from https://govtrequests.facebook.com

Freedom House. (2015). Freedom on the net. *Freedom House*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2015

Freedom House. (2016). Freedom on the net. *Freedom House*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2016

Google. (2016). *Transparency report*. Retrieved from https://www.google.com/transparencyreport/?authuser=1

Gorny, E. (2007). *The Russian internet: Between kitchen-table talks and the public sphere*. Boston, MA: Art Margins.

Greenwald, G. (2014). *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance state*. New York, NY: Henry Holt and Co.

Habermas, J. (1989). *The structural transformation of the public sphere: An inquiry into a category of bourgeois society*. Cambridge, MA: MIT Press.

Hanson, E. C. (2008). *The information revolution and world politics*. Lanham, MD: Rowman & Littlefield.

Harding, L. (2014). *The Snowden files: The inside story of the world's most wanted man*. New York, NY: Vintage Books.

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave? Digital media and the Arab Spring*. Oxford and New York, NY: Oxford University Press.

Human Rights Watch. (2017, January 17). Russia: Government vs. rights groups. *The Battle Chronicle*. Retrieved from https://www.hrw.org/russia-government-against-rights-groups-battle-chronicle

Kang, C., & Benner, K. (2017, January 6). Russia requires Apple and Google to remove LinkedIn from local App Stores. *The New York Times*. Retrieved from https://www.nytimes.com/2017/01/06/technology/linkedin-blocked-in-russia.html

Karlekar, K., & Cook, S. (2009). *Access and control: A growing diversity of threats to internet freedom*. Washington, DC: Freedom House.

Kratasjuk, E. (2006). Construction of "reality" in Russian mass media news on television and on the Internet. In H. Schmidt, K. Teubener, & N. Konradova (Eds.), *Control + shift. Public and private usages of the Russian internet* (pp. 34–50). Norderstedt: Books on Demand.

Labott, E. (2011, December 6). Clinton cites "serious concerns" about Russian election. *CNN*. Retrieved from http://www.cnn.com/2011/12/06/world/europe/russia-elections-clinton

Lokshina, T. (2016, July 7). Draconian law rammed through Russian parliament: Outrageous provisions to curb speech, privacy, freedom of conscience. *Human Rights Watch*. Retrieved from https://www.hrw.org/news/2016/06/23/draconian-law-rammed-through-russian-parliament

Luhn, A. (2014, December 12). Google to close engineering office in Russia as internet restrictions bite. *The Guardian*. Retrieved from http://www.theguardian.com/world/2014/dec/12/google-closes-engineering-office-russia

MacKinnon, R. (2011). China's "networked authoritarianism". *Journal of Democracy*, *22*(2), 32–46.

MacKinnon, R. (2012). *Consent of the networked: The world-wide struggle for Internet freedom*. New York, NY: Basic Books.

MacKinnon, R., Hickock, E., Bar, A., & Lim, H. (2014). *Fostering freedom online: The role of internet intermediaries*. Paris: UNESCO.

Maréchal, N., MacKinnon, R., Bar, A., Kumar, P., Mendes de Almeida Bottino, C. B., Micek, P., . . . Wanstreet, R. (2015). *Case study research: Laying the groundwork for the methodology*. Washington, DC: New America Open Technology Institute. Retrieved from https://rankingdigitalrights.org/wp-content/uploads/2015/02/RDR-Case-studies.pdf

Masnick, M. (2014, May 16). Russian official threatens to block Twitter and Facebook in Russia. *Tech Dirt*. Retrieved from https://www.techdirt.com/articles/20140516/06421727254/russian-official-threatens-to-block-twitter-facebook-russia.shtml

McChesney, R. W. (2013). *Digital disconnect: How capitalism is turning the Internet against democracy*. New York, NY: The New Press.

Miller, G., & Entous, A. (2017, January 6). Declassified report says Putin "ordered" effort to undermine faith in U.S. election and help Trump. *The Washington Post*. Retrieved from https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.8ec13fc7ff94

Nechepurenko, I. (2016, June 27). Edward Snowden criticizes "Big Brother" measure in Russia. *The New York Times*. Retrieved from https://www.nytimes.com/2016/06/28/world/europe/edward-snowden-criticizes-big-brother-measure-in-russia.html

Nisbet, E. (2015). *Benchmarking public demand: Russia's appetite for Information control*. Philadelphia, PA: Center for Global Communication Studies.

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111–130.

Ognyanova, K. (2015). In Putin's Russia, information has you: Media control and internet censorship. In M. M. Merviö (Ed.), *Management and participation in the public sphere* (pp. 62–78). Hershey, PA: IGI Global.

Oliphant, R. (2016, November 14). Pro-Russian candidates win presidential votes in Bulgaria and Moldova. *The Telegraph*. Retrieved from http://www.telegraph.co.uk/news/2016/11/14/pro-russian-candidates-win-presidential-votes-in-bulgaria-and-mo

Paganini, P. (2014). New powers for the Russian surveillance system SORM-2. *Security Affairs*. Retrieved from http://securityaffairs.co/wordpress/27611/digital-id/new-powers-sorm-2.html

Pearce, K. E., & Kendzior, S. (2012). Networked authoritarianism and social media in Azerbaijan. *Journal of Communication*, *62*(2), 283–298. doi:10.1111/j.1460-2466.2012.01633.x

Petrova, M., Fossato, F., Indina, T., Dokuka, S., & Asmolov, G. (2013). *Ranking digital rights report: Russia* (Unpublished Report). Moscow: Center for the Study of New Media and Society.

Pickard, V. W. (2014). *America's battle for media democracy: The triumph of corporate libertarianism and the future of media reform*. New York, NY: Cambridge University Press.

Pickard, V. W. (2017, January 30). The problem with our media is extreme commercialism. *The Nation*. Retrieved from https://www.thenation.com/article/the-problem-with-our-media-is-extreme-commercialism

Pomerantsev, P. (2014). *Nothing is true and everything is possible: The surreal heart of the new Russia* (1st ed.). New York, NY: PublicAffairs.

Pomerantsev, P. (2016). The Kremlin's information war. In L. Diamond, M. F. Plattner, & C. Walker (Eds.), *Authoritarianism goes global: The challenge to democracy* (pp. 174–186). Baltimore, MD: Johns Hopkins University Press.

Powers, S. M., & Jablonski, M. (2015). *The real cyber war: The political economy of internet freedom*. Urbana, IL: University of Illinois Press.

Price, M. E. (2015). *Free expression, globalism, and the new strategic communication*. New York, NY: Cambridge University Press.

Rohlenko, D. (2007). *The first Russian printed newspaper*. Science and Life.

Rothrock, K. (2016, October 25). Russia is reportedly banning LinkedIn. *Global Voices*. Retrieved from https://globalvoices.org/2016/10/25/russia-is-reportedly-banning-linkedin

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *International Journal of Communication*, *10*, 2221–2237.

Scott, M. (2016, November 10). Russia prepares to block LinkedIn after court ruling. *The New York Times*. Retrieved from https://www.nytimes.com/2016/11/11/technology/russia-linkedin-data-court-blocked.html?_r=0

Sharkov, D. (2016, April 14). Kremlin rebuffs Donald Trump's Edward Snowden "spy" claims. *Newsweek*. Retrieved from http://www.newsweek.com/kremlin-rebuffs-donald-trumps-snowden-claims-433332

Smith, D., & Walker, S. (2016, March 10). Former Putin press minister died of blow to head in Washington hotel. *The Guardian*. Retrieved from http://www.theguardian.com/world/2016/mar/10/mikhail-lesin-blunt-force-trauma-death-washington-dc-vladimir-putin

Soldatov, A., & Borogan, I. (2012). The Kremlin's new internet surveillance plan goes live today. *Wired*. Retrieved from https://www.wired.com/2012/11/russia-surveillance

Soldatov, A., & Borogan, I. (2013). Russia's surveillance state. *World Policy Journal*. Retrieved from http://www.worldpolicy.org/journal/fall2013/Russia-surveillance

Soldatov, A., & Borogan, I. (2015). *The red web: The struggle between Russia's digital dictators and the new online revolutionaries* (1st ed.). New York, NY: PublicAffairs.

Twitter. (2015). *Transparency report*. Retrieved from https://transparency.twitter.com/en.html

Twitter. (2016). *Transparency report*. Retrieved from https://transparency.twitter.com/en.html

White, S., & McAllister, I. (2014). Did Russia (nearly) have a Facebook revolution in 2011? Social media's challenge to authoritarianism. *Politics*, *34*(1), 72–84. doi:10.1111/1467-9256.12037

Williams, J., & Toropin, K. (2017, January 18). Russia extends Edward Snowden's asylum to 2020. *CNN*. Retrieved from http://www.cnn.com/2017/01/18/europe/russia-snowden-asylum-extension

Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), 75–89. doi:10.1057/jit.2015.5

Zuckerberg, M. (2016, November 12). *Facebook post*. Retrieved from https://www.facebook.com/zuck/posts/10103253901916271

About the Author

Nathalie Maréchal is a doctoral candidate at the University of Southern California's Annenberg School for Communication and Journalism and Senior Research Fellow at Ranking Digital Rights. She researches the intersection of internet policy and human rights, and is writing a dissertation on the political economy of digital rights technology. Nathalie's work has been published in the *International Journal of Communication*, *Media and Communication*, the *Fibreculture Journal*, and by the Global Commission on Internet Governance. She frequently speaks at international conferences about issues related to data, society and human rights.